Metrics-Based Risk Assessment and Management of Digital Forensics

M. Sahinoglu, Stephen Stockton, Robert Barclay, and Scott Morton

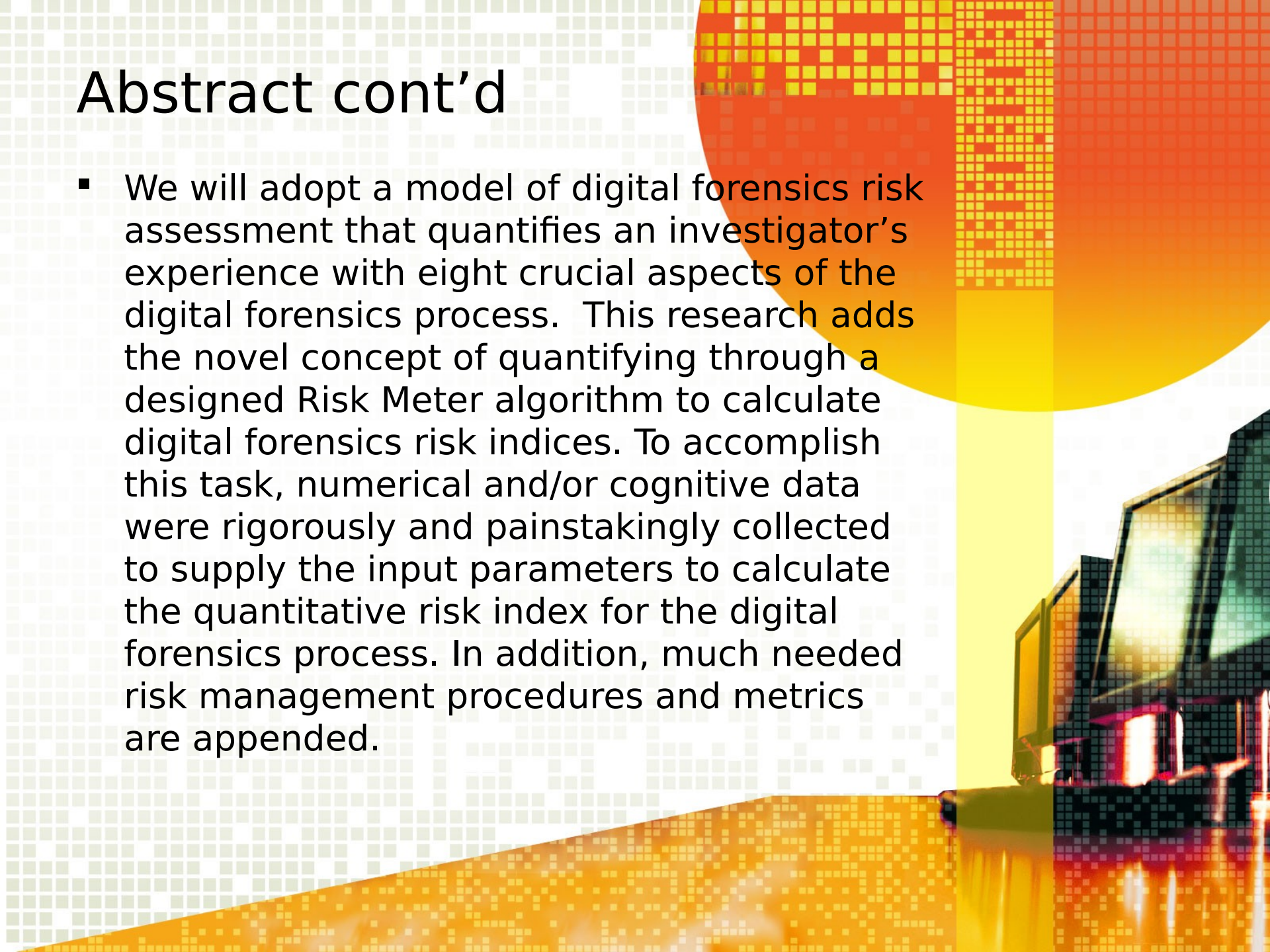
Informatics Institute, AUM, Montgomery
MeSa@aum.edu

Abstract

- Driven by the ubiquity of computers in modern life and the subsequent rise of cyber-criminality and cyber-terrorism in civilian and defense acquisition processes, Digital Forensics is an increasingly salient one. Though primarily located in the law enforcement community, Digital Forensics is increasingly practiced within the corporate world for legal and regulatory requirements such as Sarbanes-Oxley. Digital forensics risk essentially involves the assessment, acquisition, and examination of digital evidence in such a manner that legal standards of proof and admissibility are met.

Abstract cont’d

- We will adopt a model of digital forensics risk assessment that quantifies an investigator’s experience with eight crucial aspects of the digital forensics process. This research adds the novel concept of quantifying through a designed Risk Meter algorithm to calculate digital forensics risk indices. To accomplish this task, numerical and/or cognitive data were rigorously and painstakingly collected to supply the input parameters to calculate the quantitative risk index for the digital forensics process. In addition, much needed risk management procedures and metrics are appended.

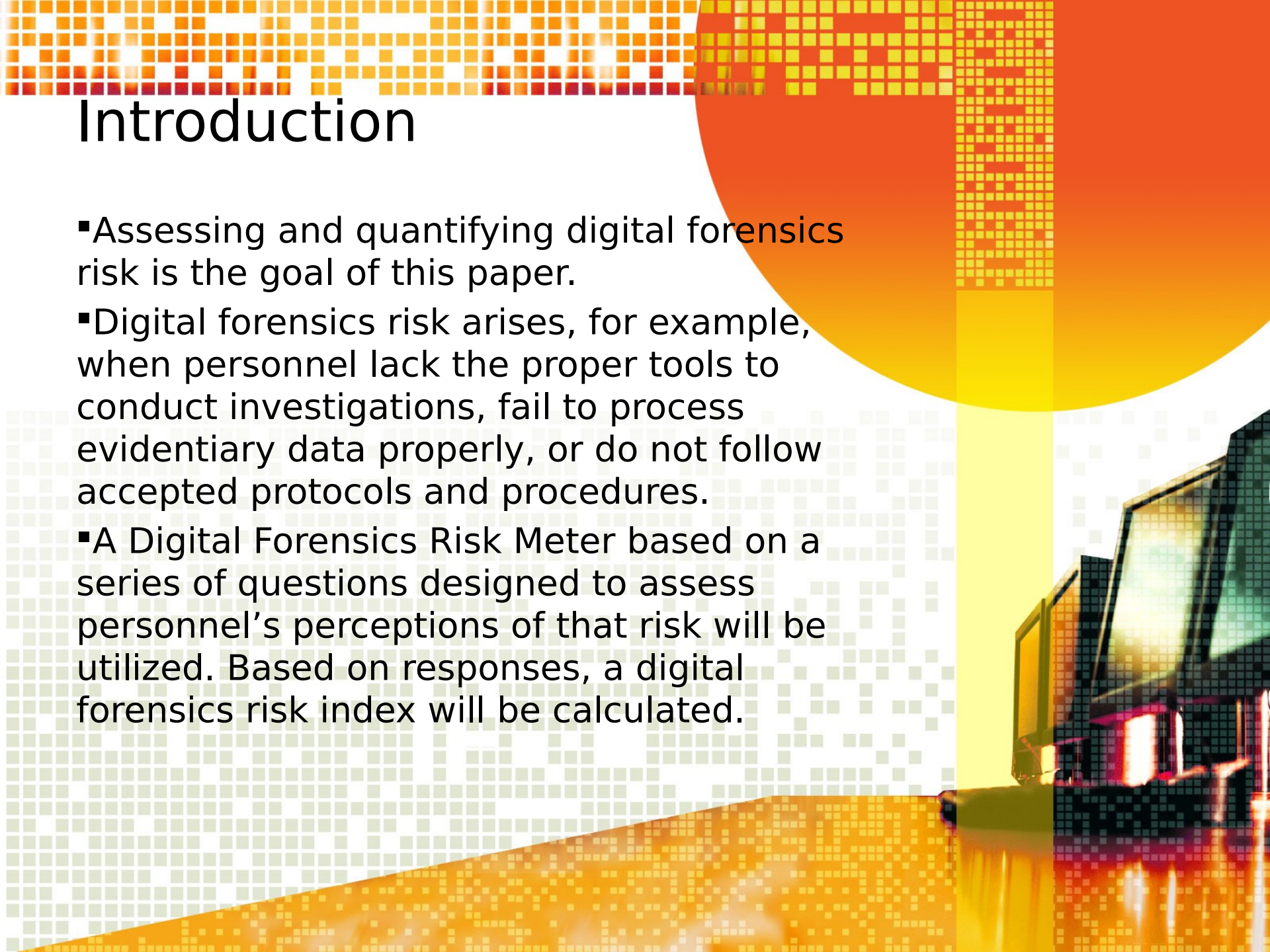


Introduction

- Digital Forensics is a topic that has been popularized by television programs such as *CSI*. Crime-solving glamour and drama aside, the reality of the digital forensics process is that it is a highly technical field that is dependent on the proper implementation of specific, well-accepted protocols and procedures. Inadequate forensic tools and technical examination, as well as lack of adherence to appropriate protocols and procedures can result in evidence that does not meet legal standards of proof and admissibility.

Introduction

- Assessing and quantifying digital forensics risk is the goal of this paper.
- Digital forensics risk arises, for example, when personnel lack the proper tools to conduct investigations, fail to process evidentiary data properly, or do not follow accepted protocols and procedures.
- A Digital Forensics Risk Meter based on a series of questions designed to assess personnel's perceptions of that risk will be utilized. Based on responses, a digital forensics risk index will be calculated.



Introduction

- The Digital Forensics Risk Meter presented in this paper will provide objective, automated, dollar-based risk mitigation advice for interested parties such as investigators, administrators, and officers of the court to minimize digital forensics risk.
- This paper will not only present a quantitative model but also generate a prototype numerical index that facilitates appropriate protocols and procedures, to ensure that legal standards of proof and admissibility are met.

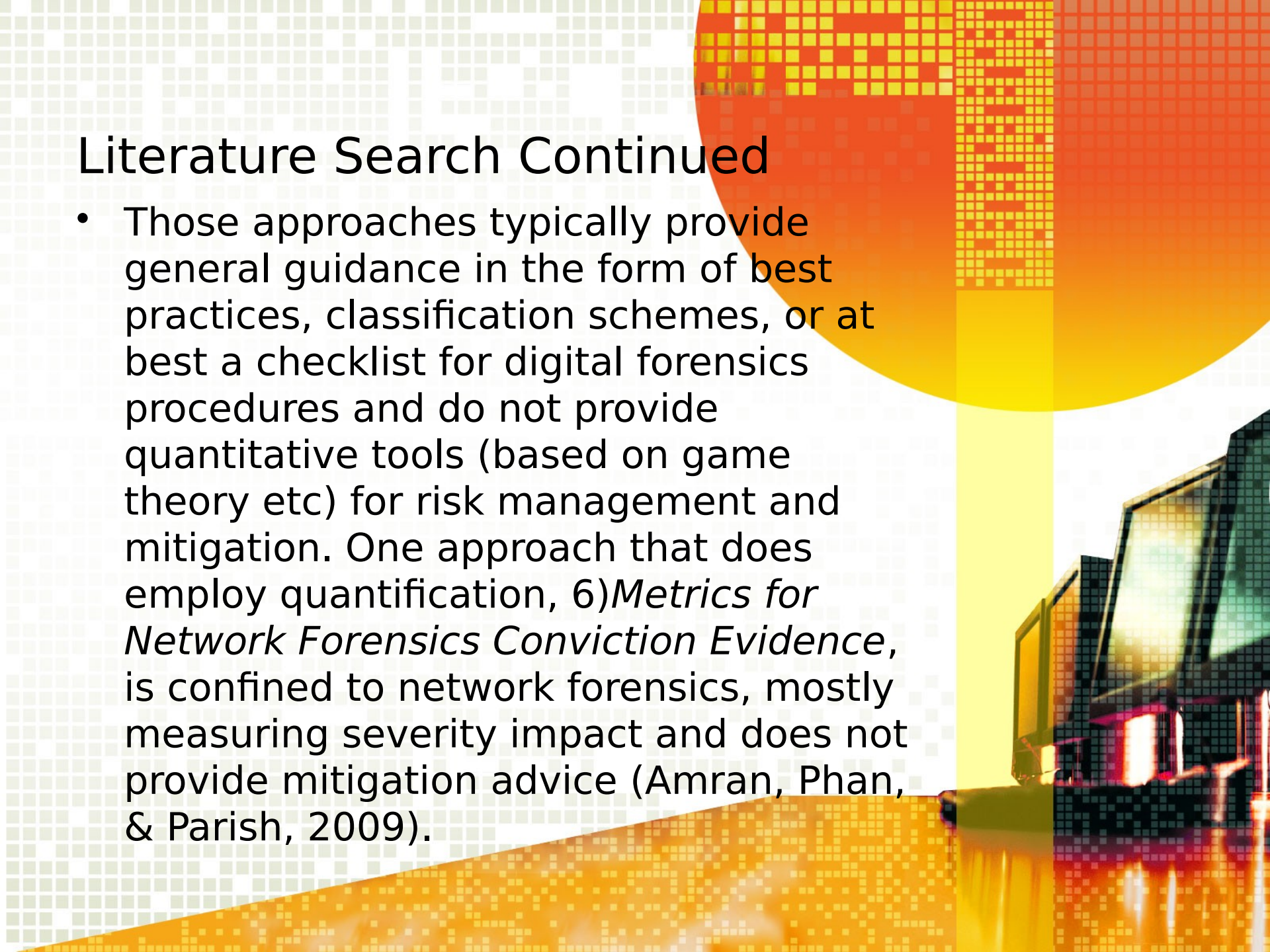
Introduction-Literature Search

- Where this approach differs from others such as:

1) US Department of Justice's *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (general guidelines and worksheets) (USDOJ, 2004), 2) E*rror, Uncertainty, and Loss in Digital Evidence* (certainty levels) (Casey, 2002), 3)*Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics* (suspicion levels) (Kim & In, 2008), 4)*Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics* (evidence reliability) (Khatir, Hejazi, & Sneiders, 2008), or 5)*Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility* (checklist) (Jones & Valli, 2011) is that:

Literature Search Continued

- Those approaches typically provide general guidance in the form of best practices, classification schemes, or at best a checklist for digital forensics procedures and do not provide quantitative tools (based on game theory etc) for risk management and mitigation. One approach that does employ quantification, 6)*Metrics for Network Forensics Conviction Evidence*, is confined to network forensics, mostly measuring severity impact and does not provide mitigation advice (Amran, Phan, & Parish, 2009).

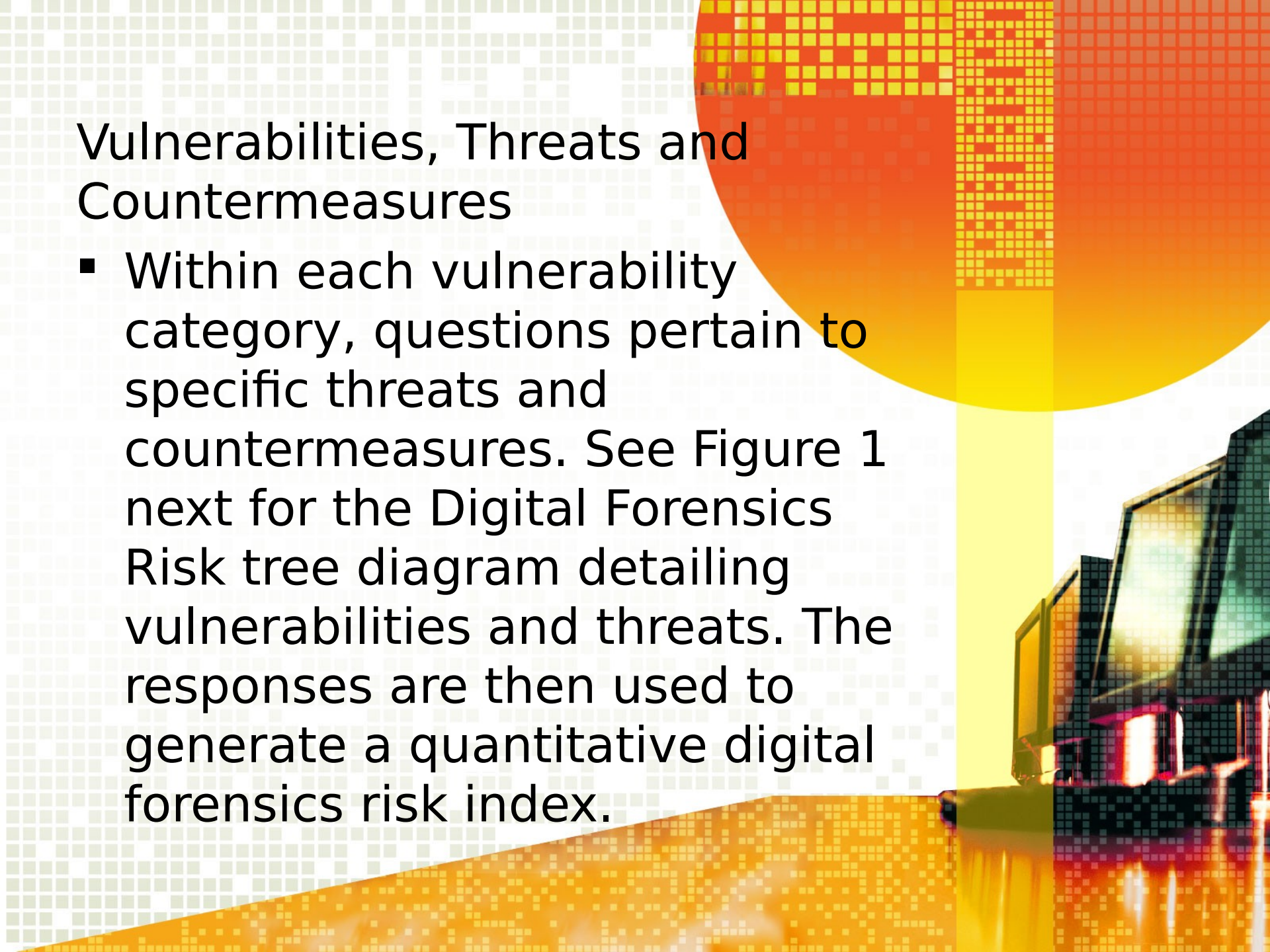


Vulnerabilities, Threats and Countermeasures

- Based on industry best practices guidelines, such as the US Department of Justice's *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, eight specific vulnerabilities are assessed: Protocols and Procedures, Evidence Assessment, Evidence Acquisition, Evidence Examination, Documentation & Reporting, Digital Forensics Tools, Legal Aspects, and Victim Relations.

Vulnerabilities, Threats and Countermeasures

- Within each vulnerability category, questions pertain to specific threats and countermeasures. See Figure 1 next for the Digital Forensics Risk tree diagram detailing vulnerabilities and threats. The responses are then used to generate a quantitative digital forensics risk index.



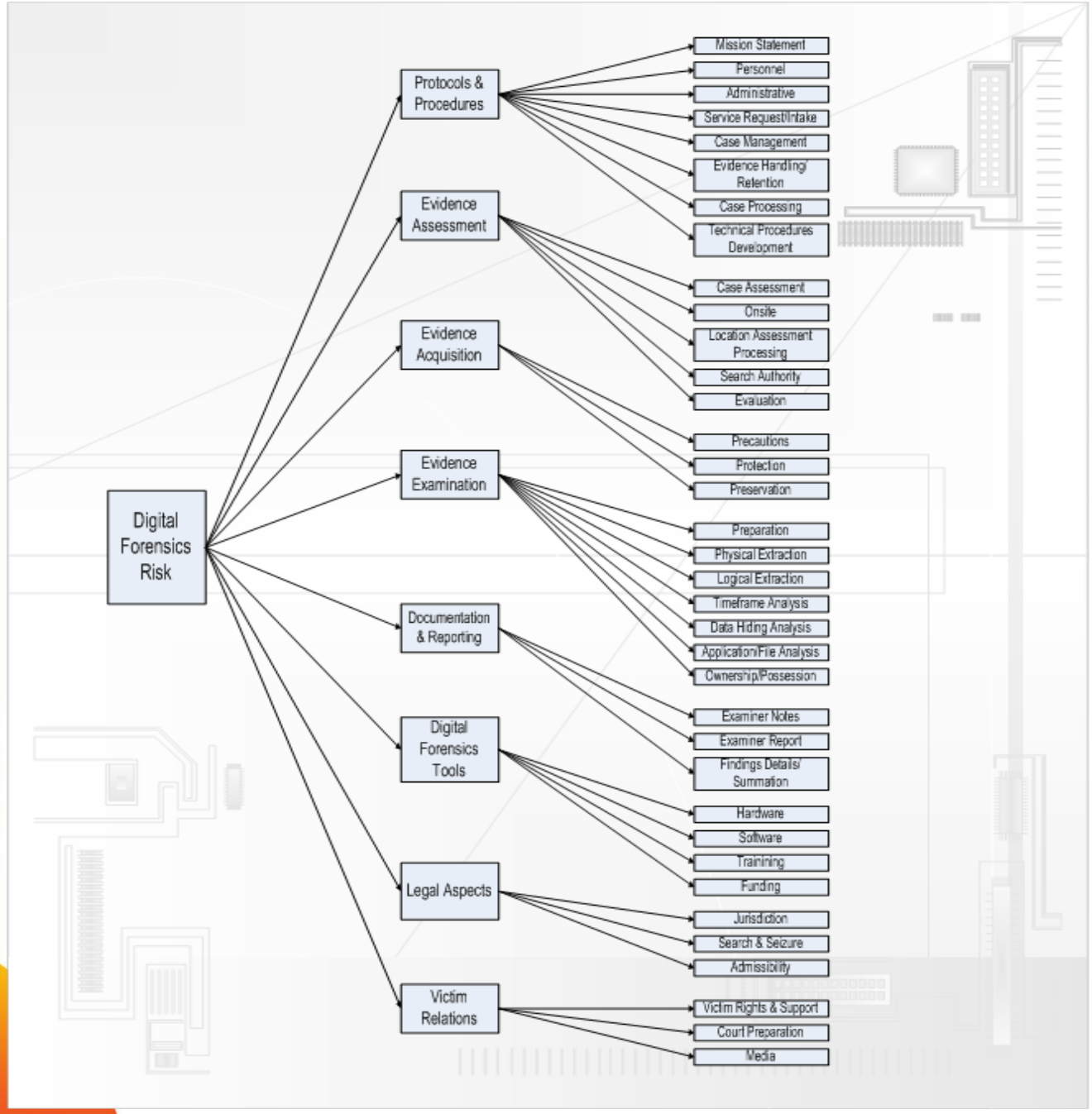


Figure 1: Digital Forensics Risk Diagram.

Assessment Questions

- Questions are designed to elicit responses regarding the perceived risk to proper digital forensics procedures, evidence handling/examination, admissibility, and other associated issues from particular threats, as well as the countermeasures the respondents may employ to counteract those threats.
- For example, in the Evidence Examination vulnerability, questions regarding the Data Hiding Analysis threat includes both threat and countermeasure questions.

Assessment Questions

Threat questions would include:

- Do file headers not correspond to file extensions?
- Did the suspect encrypt or passwords protect data?
- Are hidden messages present?
- Are host-protected areas (HPAs) present?

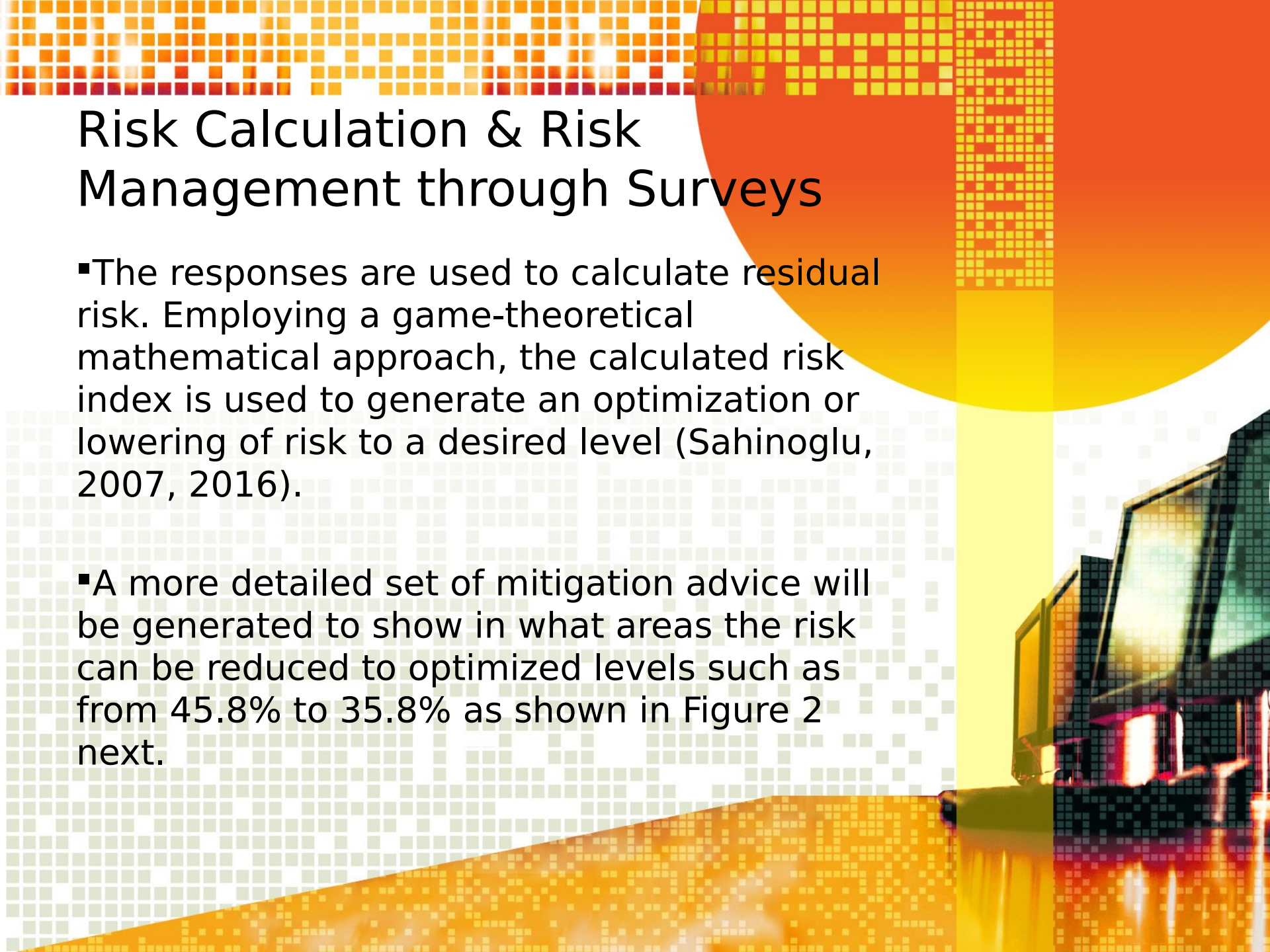
While countermeasure questions would include:

- Did the examiner correlate file headers to the corresponding file extensions to identify any mismatches which may indicate that the user intentionally hid data?
- Did the examiner gain access to all password-protected, encrypted, and compressed files, which may indicate an attempt to conceal the data from unauthorized users?
- Did the examiner conduct a thorough stenographic analysis?
- Did the examiner gain access to HPAs that may indicate an attempt to conceal data?

Risk Calculation & Risk Management through Surveys

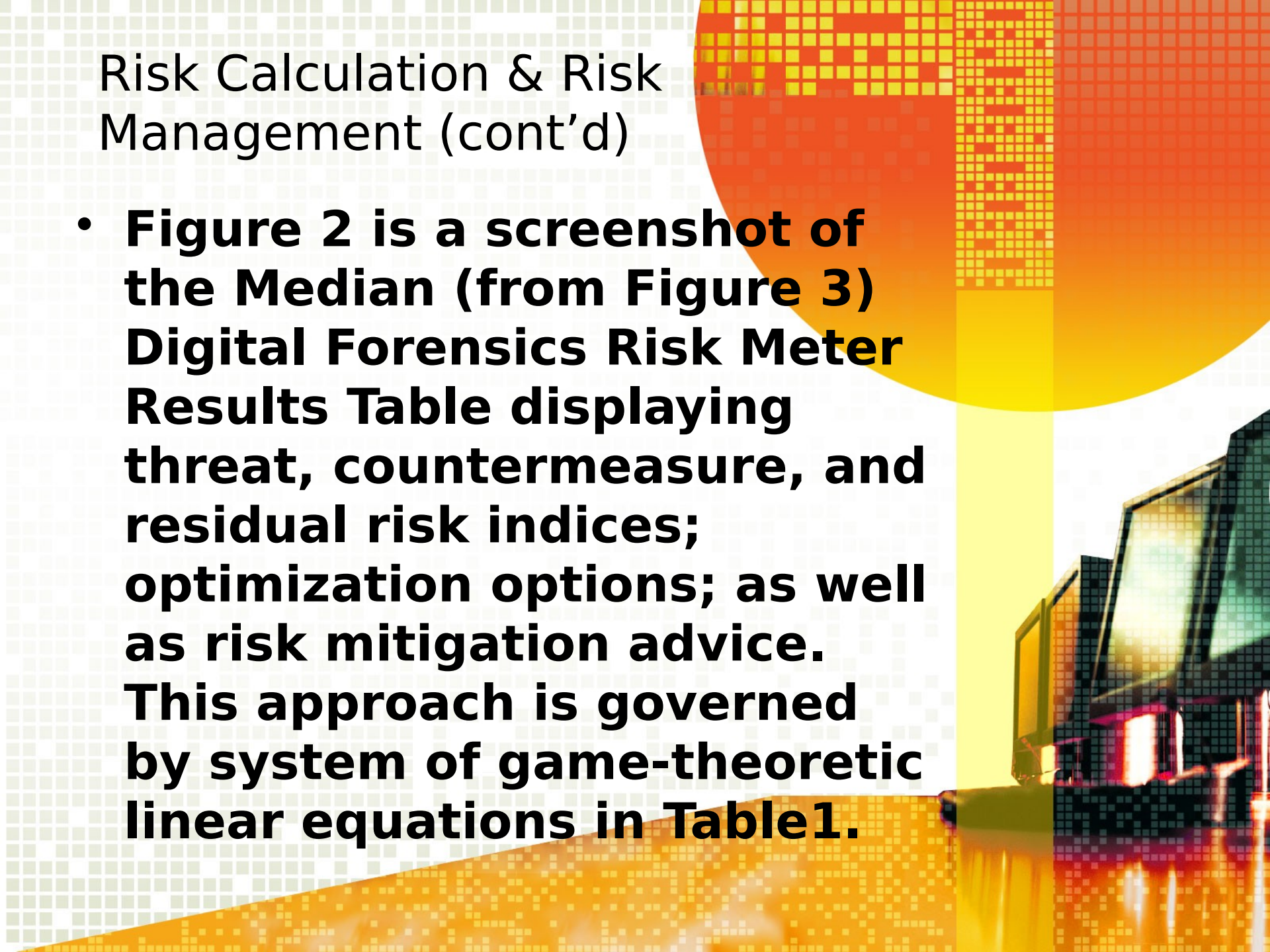
- The responses are used to calculate residual risk. Employing a game-theoretical mathematical approach, the calculated risk index is used to generate an optimization or lowering of risk to a desired level (Sahinoglu, 2007, 2016).

- A more detailed set of mitigation advice will be generated to show in what areas the risk can be reduced to optimized levels such as from 45.8% to 35.8% as shown in Figure 2 next.



Risk Calculation & Risk Management (cont'd)

- **Figure 2 is a screenshot of the Median (from Figure 3) Digital Forensics Risk Meter Results Table displaying threat, countermeasure, and residual risk indices; optimization options; as well as risk mitigation advice. This approach is governed by system of game-theoretic linear equations in Table1.**



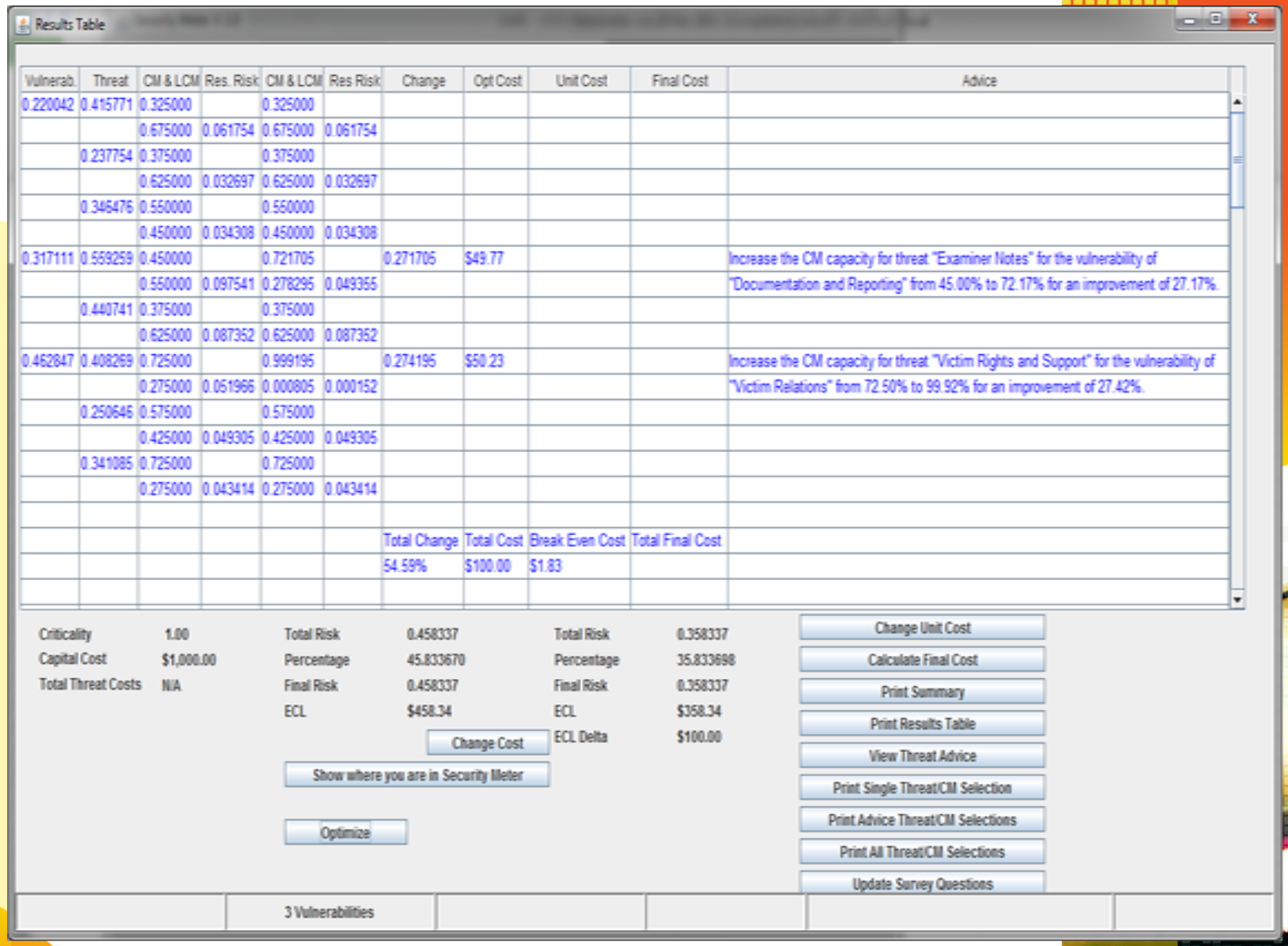
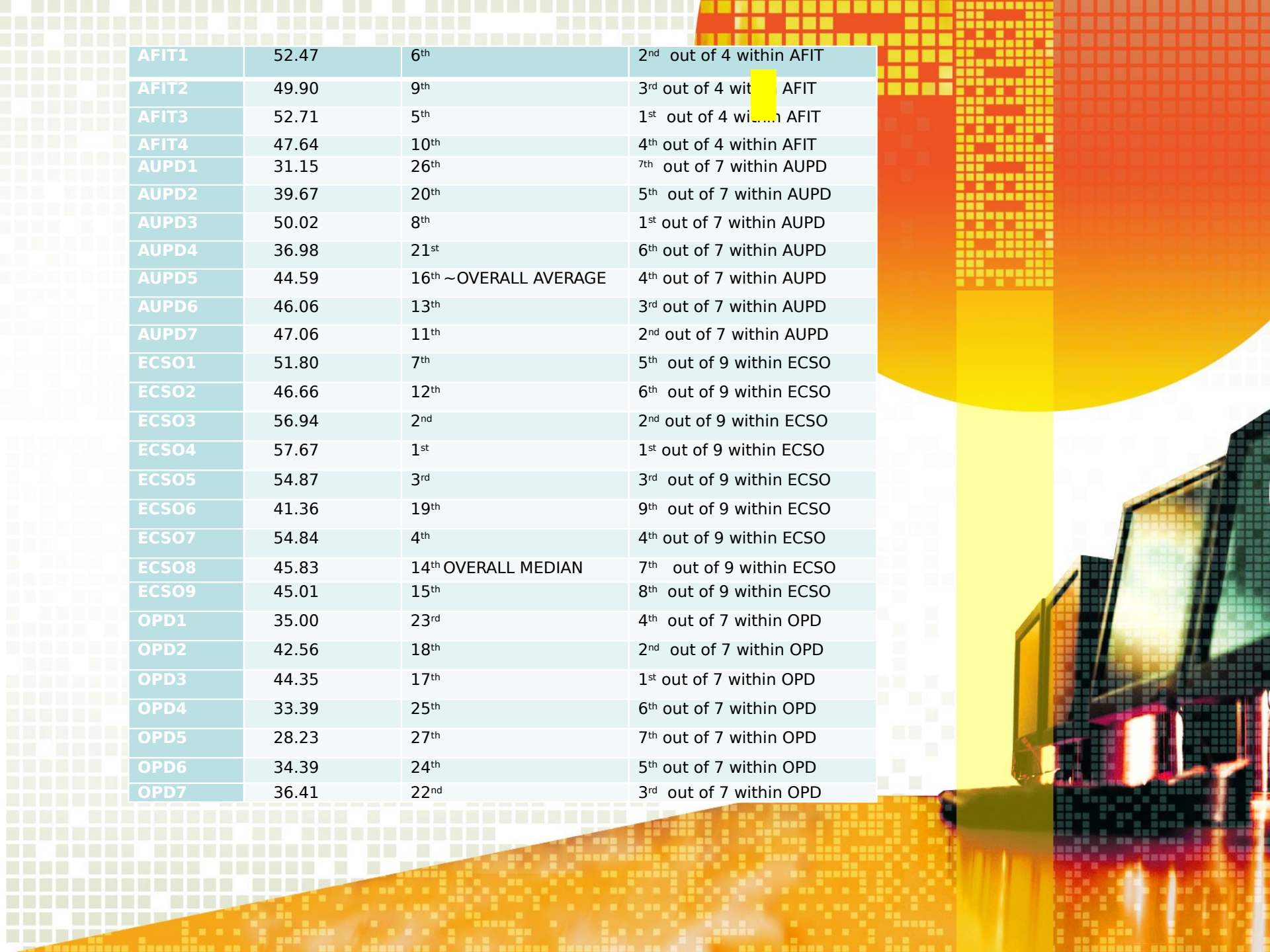


Figure 2: Median Digital Forensics Risk Meter Results Table mitigated to 35.83%. See Fig.3 for outcomes.

AFIT1	52.47	6th	2nd out of 4 within AFIT
AFIT2	49.90	9th	3rd out of 4 within AFIT
AFIT3	52.71	5th	1st out of 4 within AFIT
AFIT4	47.64	10th	4th out of 4 within AFIT
AUPD1	31.15	26th	7th out of 7 within AUPD
AUPD2	39.67	20th	5th out of 7 within AUPD
AUPD3	50.02	8th	1st out of 7 within AUPD
AUPD4	36.98	21st	6th out of 7 within AUPD
AUPD5	44.59	16th ~OVERALL AVERAGE	4th out of 7 within AUPD
AUPD6	46.06	13th	3rd out of 7 within AUPD
AUPD7	47.06	11th	2nd out of 7 within AUPD
ECSO1	51.80	7th	5th out of 9 within ECSO
ECSO2	46.66	12th	6th out of 9 within ECSO
ECSO3	56.94	2nd	2nd out of 9 within ECSO
ECSO4	57.67	1st	1st out of 9 within ECSO
ECSO5	54.87	3rd	3rd out of 9 within ECSO
ECSO6	41.36	19th	9th out of 9 within ECSO
ECSO7	54.84	4th	4th out of 9 within ECSO
ECSO8	45.83	14th OVERALL MEDIAN	7th out of 9 within ECSO
ECSO9	45.01	15th	8th out of 9 within ECSO
OPD1	35.00	23rd	4th out of 7 within OPD
OPD2	42.56	18th	2nd out of 7 within OPD
OPD3	44.35	17th	1st out of 7 within OPD
OPD4	33.39	25th	6th out of 7 within OPD
OPD5	28.23	27th	7th out of 7 within OPD
OPD6	34.39	24th	5th out of 7 within OPD
OPD7	36.41	22nd	3rd out of 7 within OPD



- **Min COLLOSS (Column loss), s. t. (subject to):**
- **CM_{11} < 1** (1), **CM_{12} < 1** (2), **CM_{13} < 1** (3), **CM_{21} <1** (4), **CM_{22} <1** (5), **CM_{31} <1** (6), **CM_{32} <1** (7), **CM_{33} <1** (8), **COLLOSS<1** (9)
- **CM_{11} > 0.675** (10), **CM_{12} > 0.475** (11), **CM_{13} > 0.725** (12),
- **CM_{21} > 0.725** (13), **CM_{22} > 0.725** (14),
- **CM_{31} > 0.675** (15), **CM_{32} > 0.675** (16), **CM_{33} > 0.675** (17),
- **0.09148 CM_{11} -1COLLOSS < 0** (18),
- **0.05231 CM_{12} -1COLLOSS < 0** (19),
- **0.07629 CM_{13} -1COLLOSS < 0** (20),
- **0.17734 CM_{21} -1COLLOSS < 0** (21)**,**
- **0.13966 CM_{22} -1COLLOSS < 0** (22**),**
- **0.18896 CM_{31} - 1COLLOSS < 0** (23),
- **0.11601 CM_{32} -1COLLOSS < 0** (24),
- **0.15787 CM_{33} -1COLLOSS < 0** (25),
- **0.09148 CM_{11} + 0.05231 CM_{12} + 0.07629 CM_{13} + 0.17734 CM_{21} + 0.13966 CM_{22} + 0.18896 CM_{31} + 0.11601 CM_{32} + 0.15787 CM_{33} > 1- 0.3583 = 1- 0.3583 = 0.6417** (26)

- *Table 1. Set of constrained linear equations for Table 1's median to attain a risk mitigated to 35.83% from an undesirable 45.83% inspired by Figure 2; where Total # Constraints=3*#Selected Threats + 2=3*8+2=24+2=26 along with Objective(Min) Function.*

Risk Calculation & Risk Management through Surveys

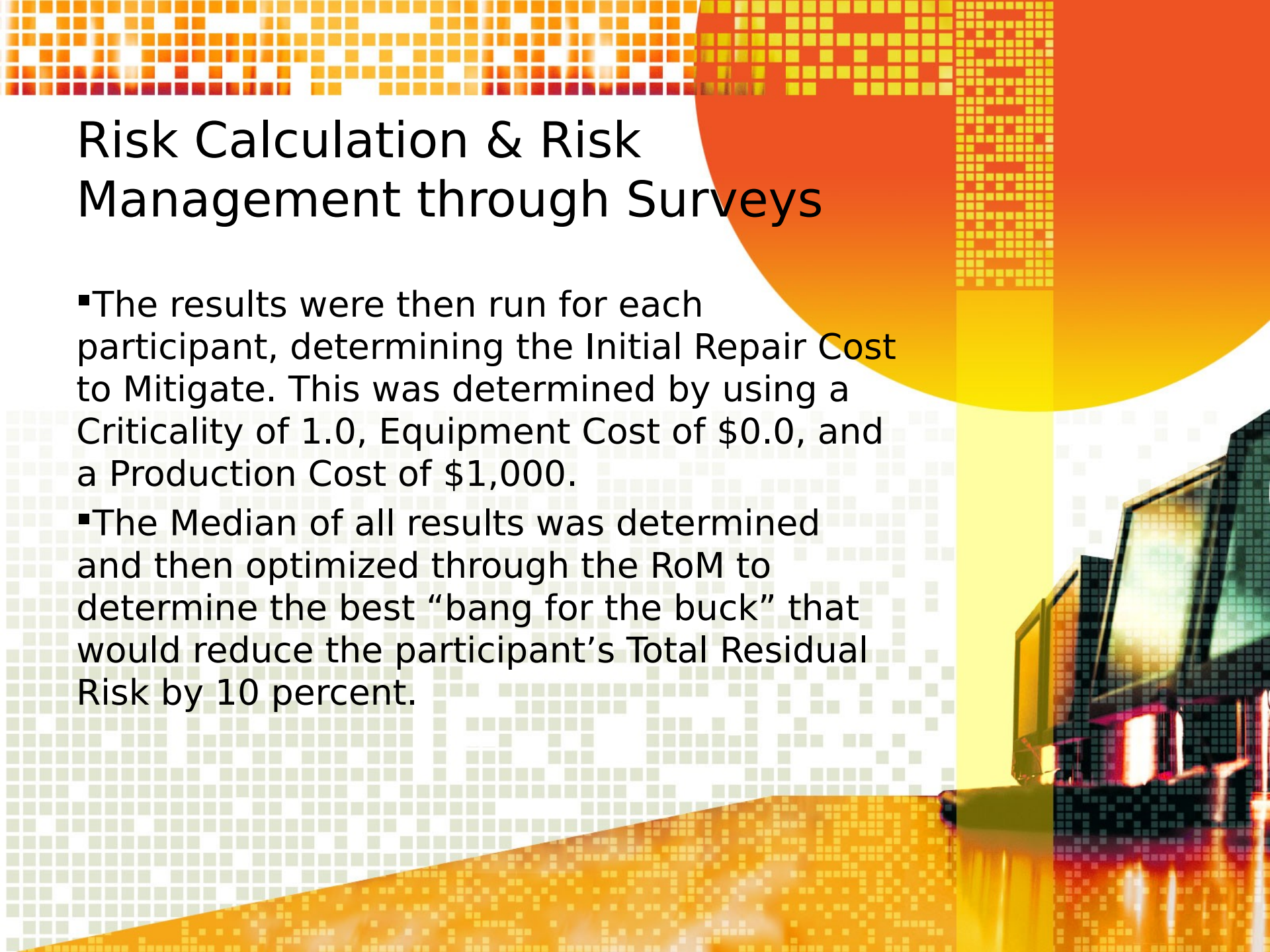
- For this study, a random sample of 27 respondents was taken and their residual risk results were tabulated.
- The survey portfolio used in this research paper for the assessment showed the complexity of the field, as one realizes digital forensics encompasses tools, procedures, specific training, budget, and trial.
- Ultimately, three law enforcement offices and one special investigation/training organization participated and provided valuable input.

Risk Calculation & Risk Management through Surveys

- Participants ranged from investigators, initial responders, digital forensics specialists, and legal experts, i.e. District Attorney Office personnel.
- The range of expertise of the participants was invaluable, as each provided insight into an aspect of the survey that is often unique to a position within a department.
- Because of this range of expertise, the authors believe they were able to capture the three main components of the survey: collection of evidence, packaging of evidence for trial, and presentation of evidence at trial.

Risk Calculation & Risk Management through Surveys

- The results were then run for each participant, determining the Initial Repair Cost to Mitigate. This was determined by using a Criticality of 1.0, Equipment Cost of $0.0, and a Production Cost of $1,000.
- The Median of all results was determined and then optimized through the RoM to determine the best “bang for the buck” that would reduce the participant’s Total Residual Risk by 10 percent.

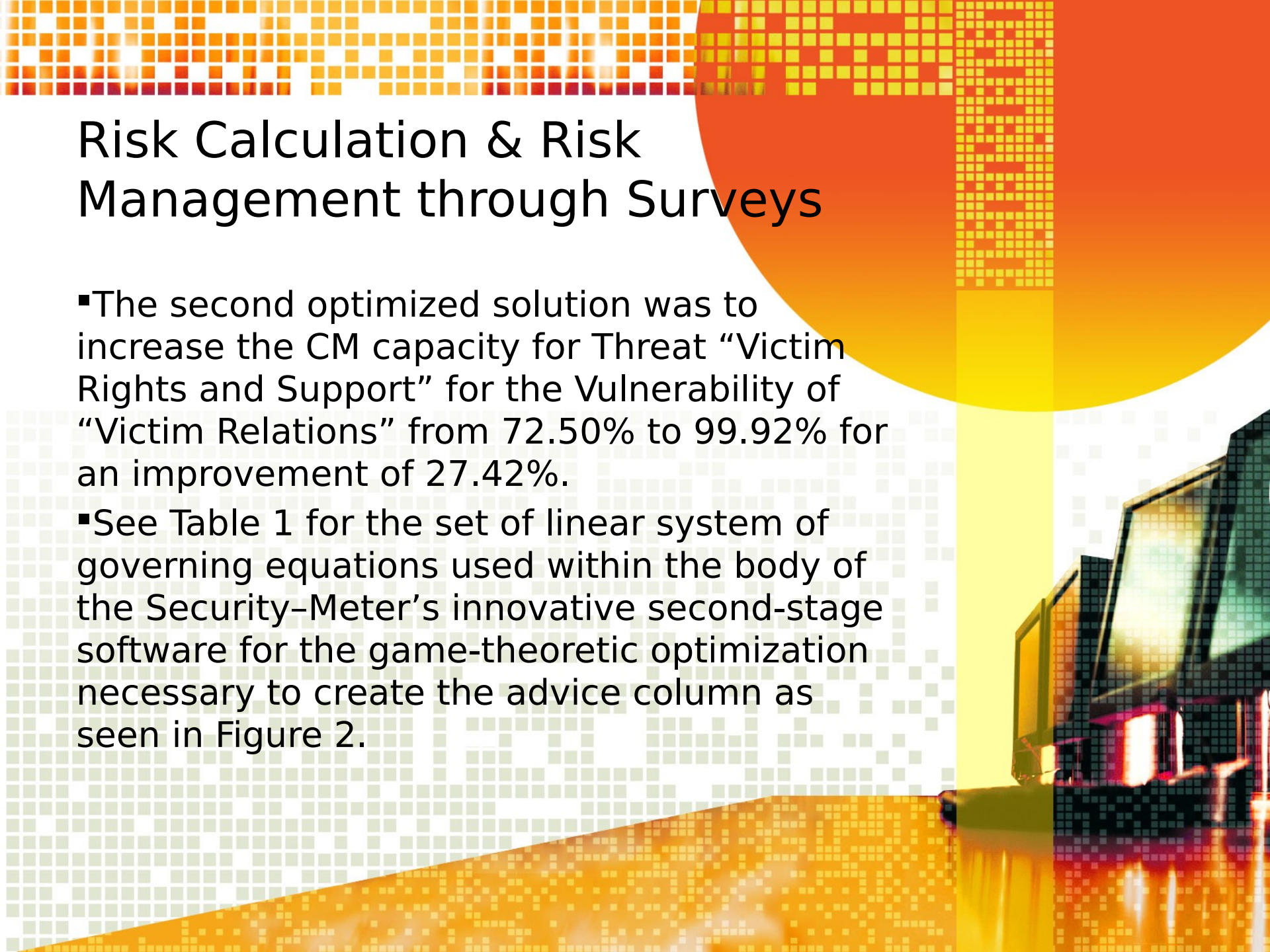


Risk Calculation & Risk Management through Surveys

- The initial Total Residual Risk for the median participant was 45.8% with an Expected Cost of Loss (ECL) of $458.34. Once optimized, the Total Risk was reduced to 35.8% and the ECL was reduced by $100 to a total ECL of $358.34 as seen in Figure 2.
- The first optimized solution was to increase the countermeasure (CM) capacity for the Threat “Examiner Notes” for the Vulnerability “Documentation and Reporting” from 45.00% to 72.17% for an improvement of 27.17%.

Risk Calculation & Risk Management through Surveys

- The second optimized solution was to increase the CM capacity for Threat “Victim Rights and Support” for the Vulnerability of “Victim Relations” from 72.50% to 99.92% for an improvement of 27.42%.
- See Table 1 for the set of linear system of governing equations used within the body of the Security–Meter’s innovative second-stage software for the game-theoretic optimization necessary to create the advice column as seen in Figure 2.



Empirical Validation of Risk Calculation & Risk Management through Surveys

- In each participant case, the company representatives seemed impressed with the results and noted the results for possible future implementation.
- One organization actually commented that they had already begun looking into increases in at least one countermeasure that was identified by the optimization!
- Clearly, this episode validated the tool and its usefulness in their eyes.

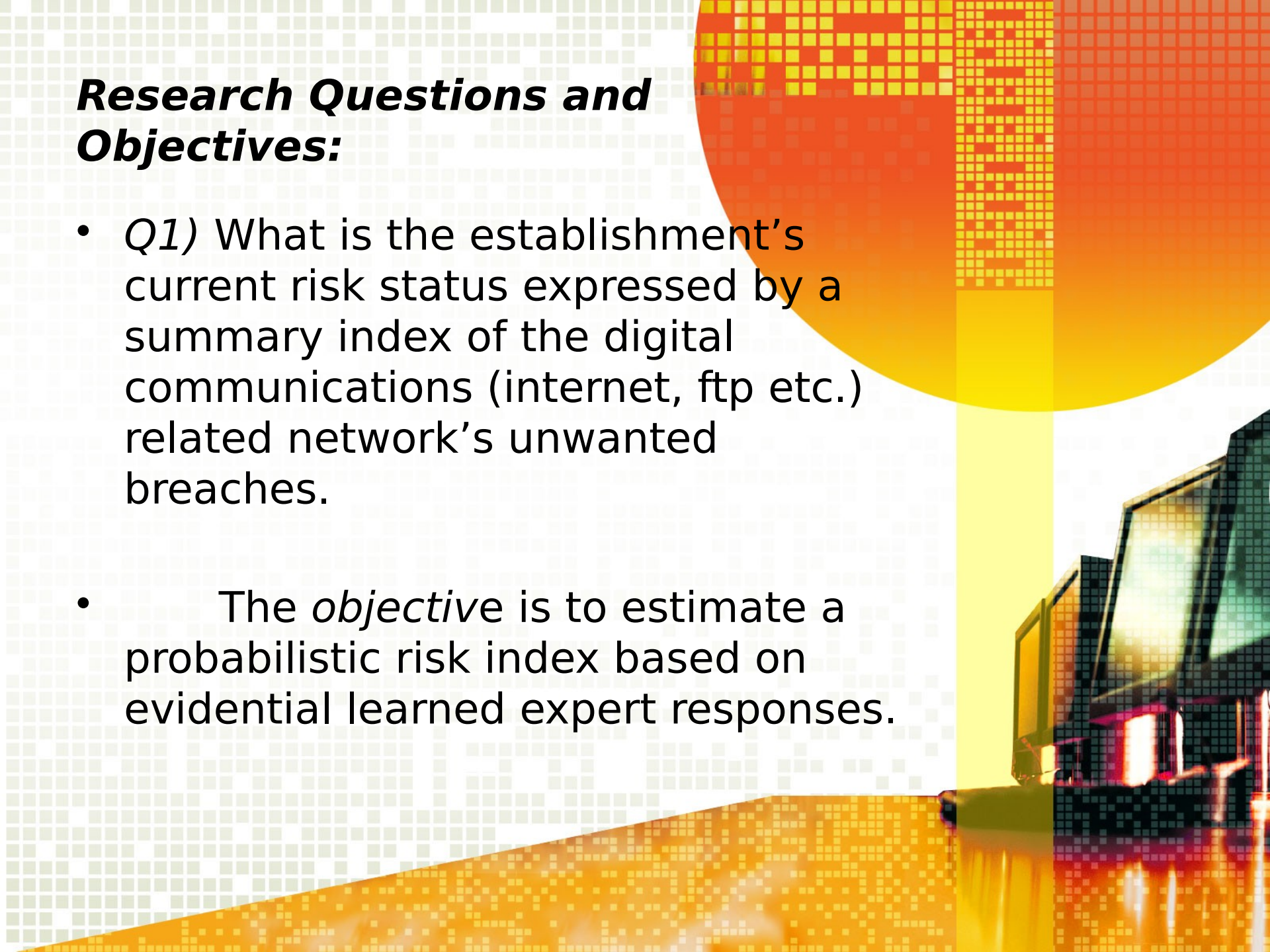
SUMMARY

- The following slides will summarize the presentation.

Research Questions and Objectives:

- *Q1)* What is the establishment's current risk status expressed by a summary index of the digital communications (internet, ftp etc.) related network's unwanted breaches.

- The *objectiv*e is to estimate a probabilistic risk index based on evidential learned expert responses.



Research Questions and Objectives:

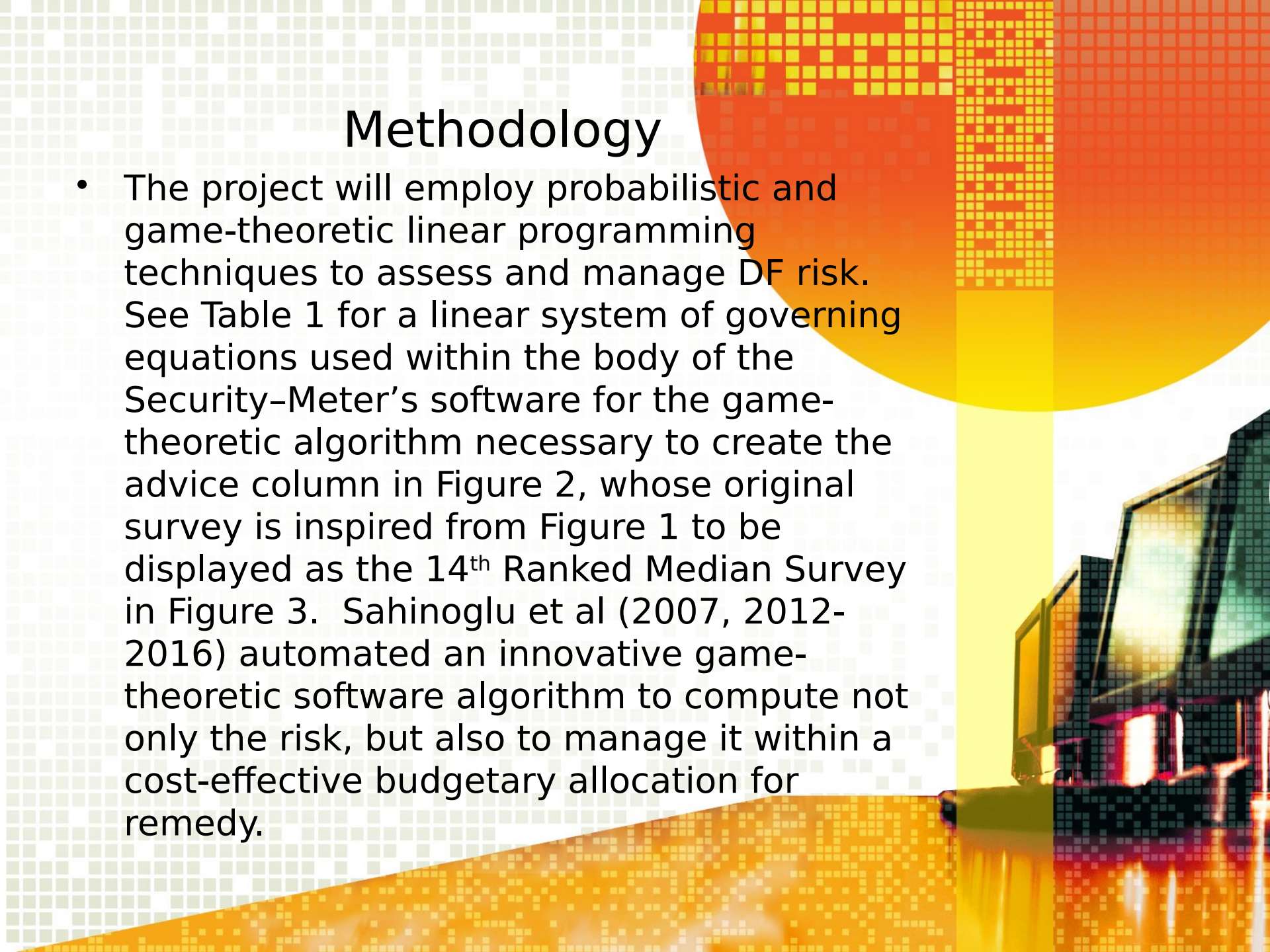
- *Q2)* What are the bottlenecks, problems and critical issues that cause the establishment to waste budgetary and human resources detected due to lower-than-standard practice by the outcomes obtained; such as the enterprise may experience 25% more Digital Forensics breaches than the set-up standards on an annual basis?
- The *objective* is to specify the problem points that one needs to mitigate to improve the digital communication system void of illegal and unethical breaches.

Research Questions and Objectives:

- *Q3)* Can the establishments specify a quasi-complete body of related vulnerabilities, threats and countermeasures to work towards the assessment of a quantifiable risk, after which a consequential dollar-based risk management remediation is pursued to make good following a related set of investments defined as countermeasures to implement.
- The *objective* is to provide guidance for cost-effective budgetary allocation plan to verify that the improvements are made. Then, a second round of remediation efforts can be executed provided an extended budget. Therefore new vulnerabilities and threats will be countermeasured.

Methodology

- The project will employ probabilistic and game-theoretic linear programming techniques to assess and manage DF risk. See Table 1 for a linear system of governing equations used within the body of the Security–Meter's software for the game-theoretic algorithm necessary to create the advice column in Figure 2, whose original survey is inspired from Figure 1 to be displayed as the 14th Ranked Median Survey in Figure 3. Sahinoglu et al (2007, 2012-2016) automated an innovative game-theoretic software algorithm to compute not only the risk, but also to manage it within a cost-effective budgetary allocation for remedy.



Discussions and Conclusion

- The advantages of conducting business on the Internet have been well documented. However this comes with the digital forensics related vulnerabilities and pertinent threats that tend to convert the positive advantages to clear disadvantages as a result of fraud and wrongdoing.
- With burgeoning information systems, digital forensics has gained worldwide momentum. In every environment, the content of digital information relative to criminal undertakings and investigation alike has vastly increased, growing disproportionately to the capacities of state and local governments as well federal and military agencies.

Discussions and Conclusion

- The risk assessment, and the risk mitigation or in general risk management that involve planned investment policy in a priority order with a sound and audition-oriented cost effective approach are missing links.
- The proposed Digital Forensics Risk Meter is an innovative initiative such that it provides a quantitative assessment of risk to the user as well as recommendations for mitigating that risk.
- This approach will be a highly useful tool to those seeking to minimize and therefore mitigate digital forensics risk by taking countermeasures obtained as an outcome of the dynamic closed-end survey.

REFERENCES

Casey, E. (2002). Error, Uncertainty, and Loss in Digital Evidence, *International Journal of Digital Evidence*, https://utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf

US Department of Justice. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Sahinoglu, M. (2007). *Trustworthy Computing*, Hoboken NJ: John Wiley

Khatir, M., Hejazi, S. M., & Sneiders, E. (2008). Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics, IEEE Proceedings of Third International Annual Workshop on Digital Forensics and Incident Analysis, WDFIA, Malaga, Spain, p. 21-29; DOI: **10.1109/WDFIA.2008.11** ce, Hoboken NJ: John Wiley

Kim, D. H., & In, H. P. (2008). Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics, Proceedings of the 2nd International Conference on Information Security and Assurance, ISA 2008. 2008. p. 193-198 4511561, Busan, Korea, Republic of

REFERENCES

Amran, A. R., Phan, R. C. W., & Parish, D. J. (2009). Metrics for Network Forensics Conviction Evidence, ICITST Internet Technology and Secured Transactions, International Conference for IEEE, p. 1-8, DOI: 10.1109/ICITST.2009.5402640

Jones, A. & Valli, C. (2011). *Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility*, Butterworth-Heinemann.

Sahinoglu, M., Cueva-Parra, L., & Ang , D. (2012) Game-theoretic computing in risk analysis, *WIREs Comput. Stat*, doi: 10.1002/wics, 1205. http://authorservices.wiley.com/bauthor/onlineLibraryTPS.asp?DOI=10.1002/wics.1205&ArticleID=961931

Sahinoglu, M., Stockton, S., Morton, S., Barclay, R., Eryilmaz, M. (2014). Assessing Digital Forensics Risk: A Metric Survey Approach, SDPS Conference Proceedings (Theme: Smart Innovative Societies), 19th International Conference on Transformative Science, Engineering Business and Social Innovation; Sarawak, Malaysia. Available at http://www.swinburne.edu.my/sdps2014

Sahinoglu M. (2016). Cyber-Risk Informatics: Engineering Evaluation with Data Science, Hoboken NJ: John Wiley